Kryptoschlüssel, Zertifikate und Smartcards in der Praxis

Für die Sicherheit bei der Datenübermittlung und -speicherung gibt es schon länger bewährte Verschlüsselungstechniken. Die unbequeme Handhabung von sicheren Passwörtern bzw. Passphrasen hat bisher ihre Anwendung für einen breiten Personenkreis unattraktiv gemacht. Die aufgekommene Diskussion über die Ausspähung von Daten und Kommunikation lässt den Wunsch nach einer einfacheren, aber nicht weniger sicheren Lösung des Problems entstehen. Der Vortrag zeigt Möglichkeiten und Grenzen, die heutige OpenSource Programme für den Einsatz von Kryptoschlüsseln, insbesondere auf Smartcards, bieten.

Die Themenbereiche sind:

- Die Auswahl der Verschlüsselungstechnik (GnuPG vs. X.509 (S/MIME))
- Welche Smartcards und welche Kartenleser funktionieren unter Linux?
- Programme mit eingebauter Unterstützung von Zertifikaten/Smartcards
- Programme, die sich mit Zertifikaten und/oder Smartcards betreiben lassen
- Live Vorführung: Wie arbeitet es sich mit einem Rechner, der für den Einsatz von Smartcards eingerichtet ist?

Anwendungen/Hilfsprogramme werden u.a. sein: firefox, thunderbird, openvpn, wpa_supplicant (WPA Enterprise), apache, dokuwiki, freeradius, libpam-pkcs11, openssh, cryptsetup, truecrypt, opensc, pcscd

Hilfreiche Vorkenntnisse sind: Grundlagen der Kommandozeile und der Verschlüsselung

Webseiten (Auswahl):

- http://www.comsafe.de/verschluesselungsverfahren.html
- http://www.kes.info/archiv/online/01-01-60-SMIMEvsOpenPGP.htm
- https://github.com/OpenSC/OpenSC/wiki (Libs für Smartcards)
- http://pcsclite.alioth.debian.org/ccid.html#CCID_compliant (Reader Software)
- http://majic.rs/book/free-software-x509-cookbook/using-x509-in-services
- http://forums.linuxmint.com/viewtopic.php?f=42&t=63376&p=364620#p364620 (Installing Mint LMDE with whole disk encryption (LUKS+LVM))
- http://people.debian.org/~rousseau/smartcard.html (Smart Card Debian Packages)
- http://ubuntuforums.org/showthread.php?t=1557180 (HOWTO: Smart Card authentication for logins, e-mail, TrueCrypt and more!)
- http://sarwiki.informatik.hu-berlin.de/Smartcard_Based_Authentication (Smartcard Based Authentication)
- http://www.linux-club.de/viewtopic.php?f=83&t=97450&start=0 (s/mime in kmail)
- http://www.linux-magazin.de/Ausgaben/2009/09/Hartes-Tuerregime/%28offset%29/8 (wpa_supplicant und 802.1X)
- http://cr.yp.to/daemontools.html (collection of tools for managing UNIX services)

und viele Man-Pages und README-Dateien zu den verwendeten Programmen und Libraries.

Zur Person: Ich beschäftige mich schon seit einiger Zeit mit den Möglichkeiten, wie Smartcards unter Linux eingesetzt werden können. Die Verfügbarkeit von Karten, Lesern und Programmen ist leider eingeschränkt. Viele Versuche waren nötig, die funktionierenden Kombinationen

herauszufinden. Ein Dank geht an die wenigen unermüdlichen Entwickler/Programmierer, die geeignete Programme erstellen. In unserer Gruppe haben wir durch den Einsatz von Zertifikaten bereits viele Dienste abgesichert, unsere Infrastruktur kann als Beispiel für Netzwerke beliebiger Größe dienen.

Rolf Wald, Vorstand LUG-Balista Hamburg e.V.